15GF1

CLERK OF CIRCUIT COURT
FILED

OCT 7 2015

TINA McDONALD, Clerk
GRANT COUNTY, WIS.

SEARCH WARRANT

STATE OF WISCONSIN)
) SS.
COUNTY OF GRANT)

In the Circuit Court of the County of Grant:

To the sheriff or any constable or any peace officer of said county or of the State of Wisconsin:

WHEREAS, Chief Terry Terpstra has this day complained in writing to the said Court, upon oath, for issuance of a search warrant to search evidence obtained in the execution of a search warrant on October 6, 2015 at 317 ½ S. Main Street, Cuba City, Wisconsin, including the following:

1. All computers and computer hardware devices, consisting of all such equipment that can collect, analyze, create, display, convert, conceal, record or transmit electronic, magnetic, optical, or similar computer or electronic impulses or data, to include, but not limited to, desktop, laptop, hand-held or tablet computers, PDA's (Personal Data Assistants), cellular/digital telephones, digital video game consoles, digital audio recorders or players (such as iPods or other similar devices), digital video recorders, microphones, digital cameras and camcorders of any size and type located by the search team, including but not limited to "web cams."

2. Internal and peripheral digital/electronic storage devices, including but not limited to internal and external hard drives, floppy disks, zip disks, CD ROM and CD-RW disks, DVD and DVD-RW disks, data cartridges, compact flash memory cards, memory sticks, thumb or flash drives, video tapes, audio tapes and other magnetic or optical memory storage devices; peripheral input/output devices, such as computer keyboards, printers, fax machines, digital cameras, scanners, video display monitors, and optical readers; reproducing devices capable of interfacing with computers and related communication devices that can be used to transmit or receive information to or from a computer; optical pick-up devices; recording devices and all associated wiring.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Any and all user manuals or instructions for use (whether in printed documentary form or digital form) for computer hardware devices or peripheral devices or computer input or output devices. Any and all user manuals (whether in printed documentary form or digital form) for any software programs known to be, or believed to be, installed on the seized computer hardware devices. Any software installation disks or system/software recovery disks.

5. Any digital, printed or written material displaying, or believed to contain, passwords, access codes, usernames or other identifiers necessary to access, examine, or operate seized devices or software seized or known or believed to be present on any seized device.

THIS SEARCH WARRANT FURTHER AUTHORIZES law enforcement/the state to:

6. Seize and remove from the premises any computers, computer storage media and any other electronic device of a type described above in order that they may be forensically analyzed at a law enforcement facility now or at a later date in order to examine the contents for contraband or other evidence.

7. Obtain full forensic copies of the contents of the hard drive(s) or internal storage media or operating system of any seized device and the contents of any seized external storage media, for the purpose of permitting and conducting a full or partial computer forensic analysis of the same.

8. Conduct a full or partial forensic examination/analysis of the devices or the contents of the devices using accepted computer forensic examination tools and techniques, for the purpose of locating, documenting, preserving and/or determining the presence or absence on or in the device of, but not limited to, the following:

   a. Evidence of who used, owned, or controlled the device at the time the things described in the warrant or relevant to the investigation were created, edited, deleted or accessed, such as logs, registry entries, configuration files, saved usernames and passwords, documents, Internet browsing histories, user profiles, email content, email contacts, "chat" and/or instant messaging content, "chat" and/or instant messaging logs, photographs, correspondence and other documents created by or saved on the computer;

   b. Evidence of the presence of malicious software that would allow others to control the computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

   c. Evidence of the lack of malicious software on the device;

   d. Evidence of the attachment to the computer or digital/electronic device of other storage devices or similar containers for electronic evidence;

   e. Evidence of the presence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer or device, or the past presence of such software on the computer or device;

   f. Evidence of the times the computer or device was used;

   g. Passwords, encryption keys, and other access devices that may be necessary to access the computer or device;

h. Documentation and manuals that may be necessary to access the computer or device or to conduct a forensic examination of the computer or device;

i. Contextual information identifiable by the analyst and necessary or helpful to understand the evidence otherwise described in this attachment.

j. Records and things evidencing the use by the device of any of the Internet Protocol (IP) addresses mentioned in the sworn affidavit/complaint supporting issuance of this search warrant in order for the computer or device to have accessed the Internet and or communicated across the Internet at all times relevant to the present investigation, including:

   i. Records of Internet Protocol addresses used by the computer or device;

   ii. Records of Internet activity by or through the computer or device, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the computer or device user entered into any Internet search engine, and records of user-typed web addresses as well as all data available on or in, or through forensic analysis of, any seized routers, modems, or network equipment used to connect to the Internet and/or other computer networks reflecting Internet or network connection history or activity.

k. Computer or digital programs or files containing, believed to contain or capable of containing images, "still" photographs, and/or digital videos, or any remnants thereof and any evidence or "meta-data" about any such files or file remnants, all regardless of file format or file name.

AND WHEREAS, Chief Terry Terpstra has further sought authority to search the above-described evidence, which may contain evidence of a crime: Possession of Child Pornography, committed in violation of Section 948.12 of the Wisconsin Statutes and which things are set forth in Chief Terry Terpstra's affidavit and are approved of by the court and set forth specifically below,

NOW, THEREFORE, in the name of the State of Wisconsin, you are commanded to search the premises described herein and return this warrant within 48 hours of the completion of the search to the Circuit Court for Grant County, to be dealt with according to law.

Dated this 6th day of October, 2015.

BY THE COURT:

Robert P. VanDeHey

The Honorable Robert P. VanDeHey

Grant County Circuit Court, Branch I

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

STATE OF WISCONSIN)
)ss
COUNTY OF GRANT)

In the Circuit Court
of the County of Grant

Terry Terpstra, being first duly sworn, on oath, states the following:

1. I am the Chief of Police for the City of Cuba City Police Department in Grant County, Wisconsin.

2. On October 6, 2015, affiant and other law enforcement, executed a search warrant at 317 ½ S. Main Street, Cuba City, Wisconsin, a residence occupied by Richard Geasland.

3. Affiant knows that the search warrant authorized the seizure of items which were or could contain evidence of a crime, specifically, possession of child pornography in violation of Chapter 948, Wis. Stats.

4. Affiant knows that Richard Geasland was present when the search warrant was executed and made statements such as there being evidence on an external hard drive which would put him away for a long time. Affiant knows that an external hard drive was seized.

5. Affiant knows that the original report related to Richard Geasland and used to secure the first search warrant, related to statements made to Susan Leppert that there were photos of naked children on the computer and that he did not want her to judge him before he could explain himself. Affiant knows that two tower drives were seized.

6. Affiant knows that numerous other electronic devices were found.

7. Affiant wishes a search warrant to search all of the electronic devices seized in the execution of the search warrant so that they may be analyzed to determine if they contain evidence of crimes, including, possession of child pornography in violation of Chapter 948, Wis. Stats.

Terry Terpstra, Affiant

STATE OF WISCONSIN)
)ss
COUNTY OF GRANT)

Terry Terpstra, being first duly sworn, on oath, says that he is the affiant above named, that he has read the foregoing affidavit and knows the contents thereof, and that the same is true to his own knowledge, except as to those matters therein stated upon information and belief, and as to those matters he believes it to be true.

Terry Terpstra, Affiant

Subscribed and sworn to before me on October 6, 2015.

Lisa A. Riniker, Notary Public
Grant County, Wisconsin.
My commission is permanent.